US008863280B1

(12) **United States Patent**
Pennington et al.

(10) **Patent No.: US 8,863,280 B1**
(45) **Date of Patent: *Oct. 14, 2014**

(54) **AUTOMATIC RESPONSE CULLING FOR WEB APPLICATION SECURITY SCAN SPIDERING PROCESS**

(71) Applicant: **WhiteHat Security, Inc.**, Santa Clara, CA (US)

(72) Inventors: **William Pennington**, San Jose, CA (US); **Jeremiah Grossman**, San Jose, CA (US); **Robert Stone**, Mountain View, CA (US); **Siamak Pazirandeh**, Santa Clara, CA (US)

(73) Assignee: **Whitehat Security, Inc.**, Santa Clara, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **13/732,554**

(22) Filed: **Jan. 2, 2013**

Related U.S. Application Data

(63) Continuation of application No. 11/864,749, filed on Sep. 28, 2007, now Pat. No. 8,370,929.

(60) Provisional application No. 60/827,407, filed on Sep. 28, 2006.

(51) **Int. Cl.**

G06F 11/00	(2006.01)
H04L 29/06	(2006.01)
G06F 21/57	(2013.01)

(52) **U.S. Cl.**
CPC ***H04L 63/1433*** (2013.01); ***G06F 21/577*** (2013.01)
USPC **726/22**; 726/4; 726/25; 713/187; 713/188; 713/189

(58) **Field of Classification Search**
CPC H04L 63/1433; H04L 63/20; H04L 67/02; G06F 21/577; G06F 2221/2119
USPC 726/25
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

7,237,265	B2	6/2007	Reshef et al.	
2003/0233581	A1*	12/2003	Reshef et al.	713/201
2005/0262063	A1*	11/2005	Conboy et al.	707/3

OTHER PUBLICATIONS

Pandey et al. "WIC: A General Purpose Algorithm for Monitoring Web Information Sources", VLDB Conference, Canada 2004, pp. 360-371.*

Pandey, et al., "WIC: A General Purpose Algorithm for Monitoring Web Information Sources", VLDB Conference, Canada 2004, pp. 360-371.

* cited by examiner

Primary Examiner — Shewaye Gelagay
(74) *Attorney, Agent, or Firm* — Davis Wright Tremaine LLP

(57) **ABSTRACT**

A method of testing a web application, wherein a web application is a program that operates on a server and interacts with clients that access the program over a network, wherein further the web application accepts parameters that define results generated from the web application, the method comprising determining which web application uniform resource identifiers (URIs) are used to access various web applications on a system, determining if more than a threshold of the URIs are for a common web application, selecting a subset of less than all of the URIs for the common web application when the threshold is exceeded for that common web application, wherein the subset is selected at least in part independently of the order generated and performing a security scan on the selected subset.

16 Claims, 4 Drawing Sheets